# **Benign**

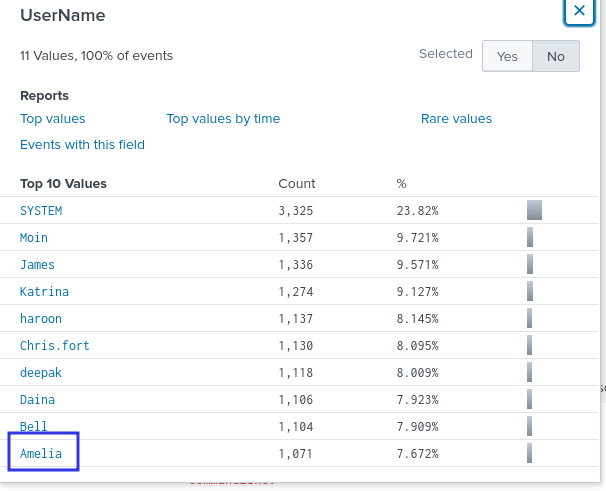
**How many logs are ingested from the month of March, 2022?**

Search for the index ; index=win\_eventlogs

13959

**Imposter Alert: There seems to be an imposter account observed in the logs, what is the name of that user?**

Check all the usernames using the username option in the left side panel , the new username which is not present in the given list and the one name which looks as legitimate but not instead of l they used 1 in that username

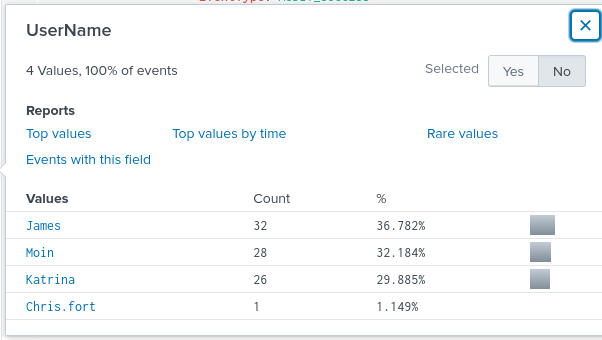


Amel1a

**Which user from the HR department was observed to be running scheduled tasks?**

I used the word schtasks to search for the scheduled tasks ; index=win\_eventlogs schtasks

And see the usernames that appear using the left side panel



From the given list which users are belongs to the HR department

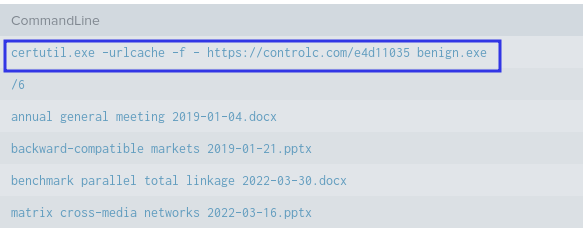
The first 3 username from the screen shot are part of IT department , and the remaining Chris.fort is HR (chris)

Chris.fort

**Which user from the HR department executed a system process (LOLBIN) to download a payload from a file-sharing host.**

Try to check the activity of each user in the HR department , first i checked for the username haroon , and the command executed by that user

index=win\_eventlogs UserName=haroon| rare limit=30 CommandLine



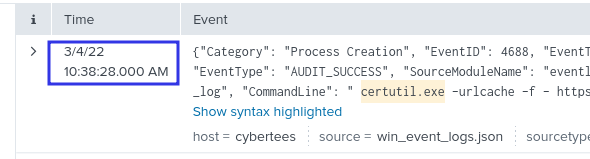
Haroon

**To bypass the security controls, which system process (lolbin) was used to download a payload from the internet?**

From previous screen we can see that the file was certutil.exe

**What was the date that this binary was executed by the infected host? format (YYYY-MM-DD)**

Search for the payload certutil.exe from the search bar



Change it to the required format and the answer will be 2022-03-04

**Which third-party site was accessed to download the malicious payload?**

Refer to the same command from the previous log

controlc.com

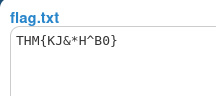
**What is the name of the file that was saved on the host machine from the C2 server during the post-exploitation phase?** Same as above benign.exe

**The suspicious file downloaded from the C2 server contained malicious content with the pattern THM{..........}; what is that pattern?**

Just visit the url which we found in the previous log



And the flag is



THM{KJ&\*H^B0}

**What is the URL that the infected host connected to?**

The url which we found in the last log

https://controlc.com/e4d11035